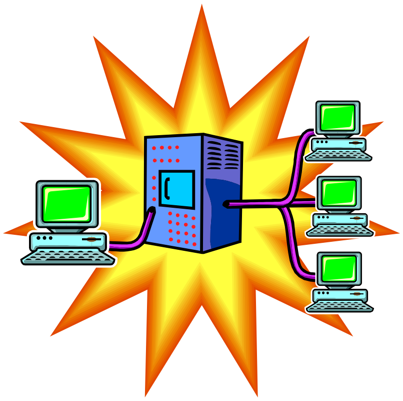
SPAWAR
Systems Center Charleston

DoD PKI

Server Certificate Enabling For

Microsoft Internet Information Server 4.0

Step 1: Generating a Key Pair and Requesting a Certificate



PK-Enabling For
Microsoft Internet Information Server
(IIS 4.0)

Step 1: Generating a Key Pair and Requesting a Certificate

This Document details how to generate a PKI key pair and request a server certificate using Microsoft Internet Information Server 4.0. It covers step 1 of a 2-step process. “Server Certificate Enabling for Microsoft Internet Information Server 4.0: Step 2: Obtaining/Installing a PKI Certificate” is a follow-up document. It details how to obtain and install a PKI server certificate as well as how to make the web server secure (https).

Step 1: Generating a Key Pair and Requesting a Certificate

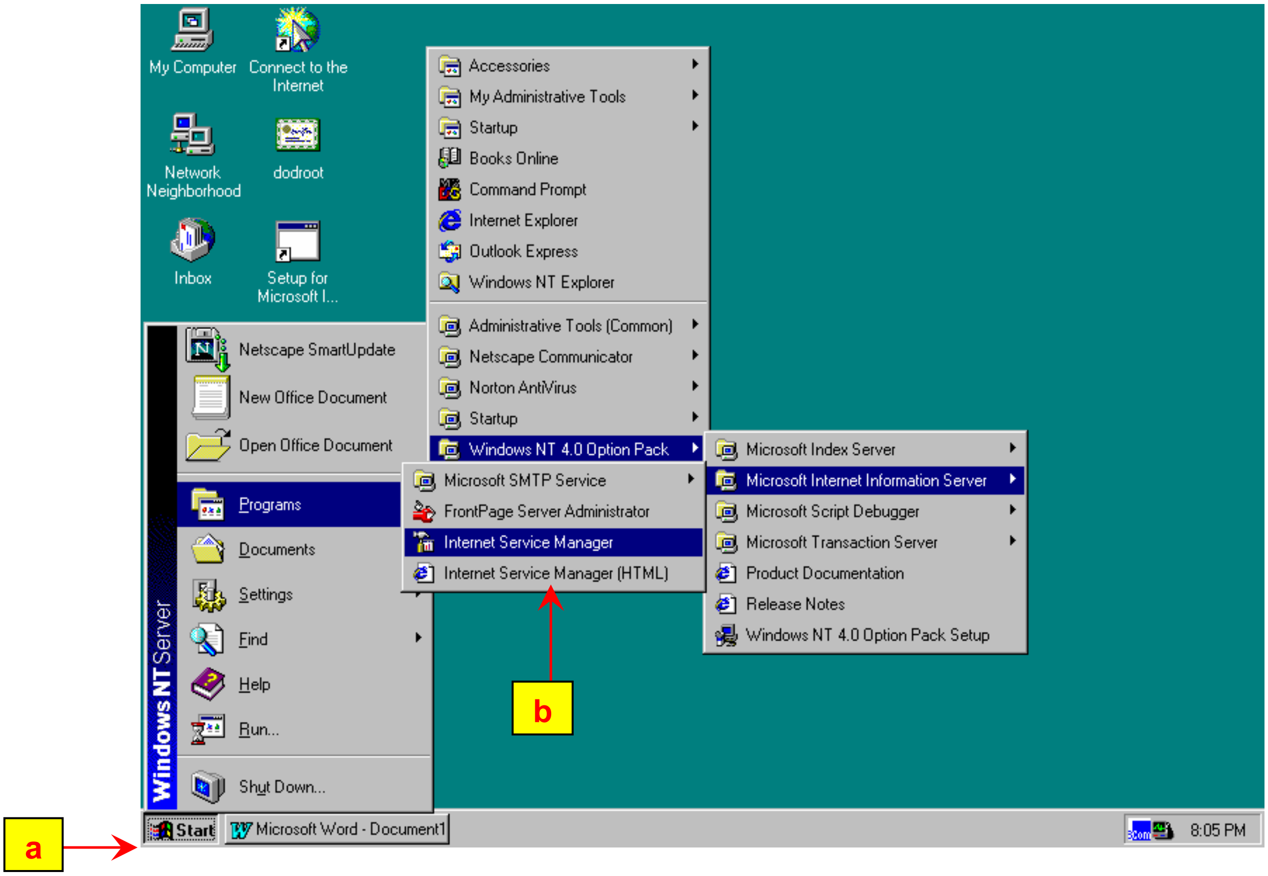
NOTE: If you are have already received your Server Certificate Approval and your Certificate Serial Number (CSN) from your RA/LRA, but have not received “Server Certificate Enabling For Microsoft Internet Information Server 4.0 Step 2” please contact Inga George, georgei@spawar.navy.mil.

PK-Enabling For Microsoft Internet Information Server (IIS 4.0)

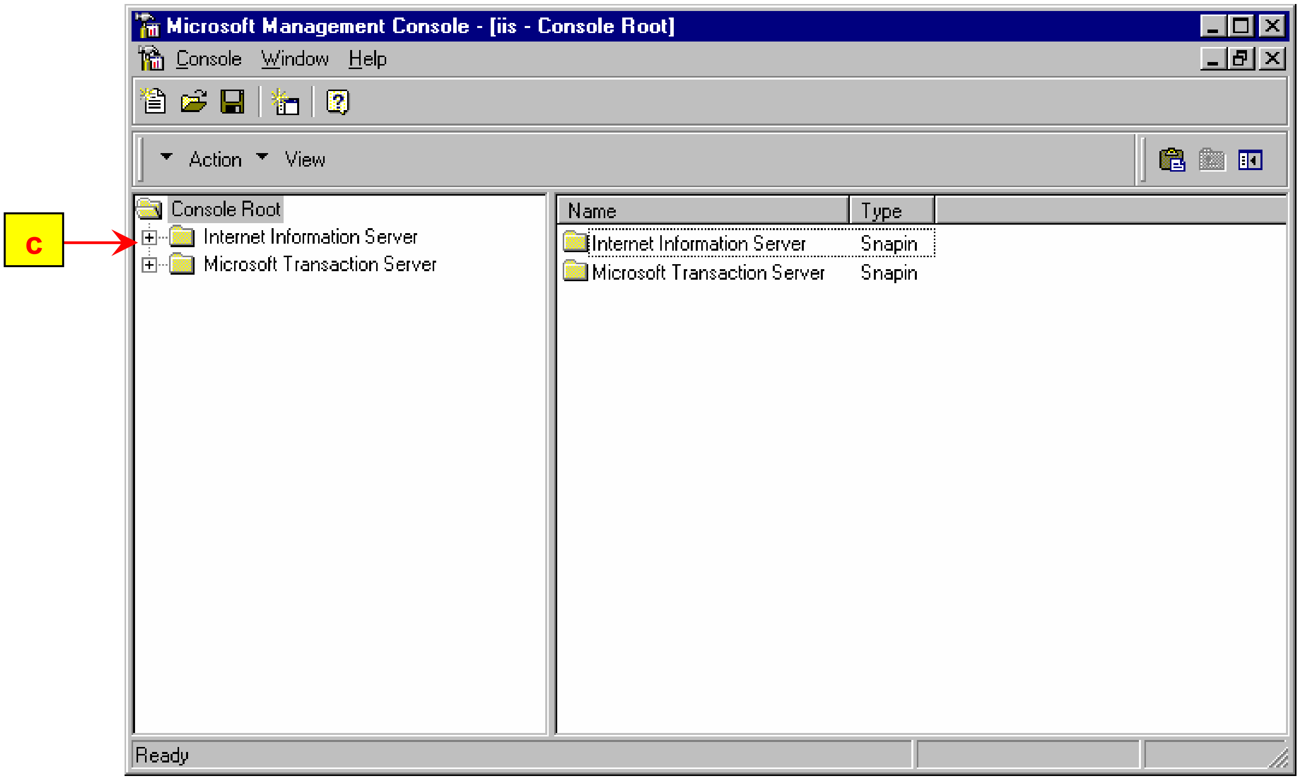
The following must be installed before attempting to install DoD certificates onto your server. **ALL SOFTWARE LISTED BELOW MUST BE 128-BIT.

1. Windows NT 4.0 Option Pack with IIS
2. Netscape 4.5 or greater
3. IE 5.0 or greater
4. Service Pack 5 is applied after all other software is installed.

1. Generating a Key File.
   a) Click **Start**
   b) **Programs**, **Windows NT 4.0 Option Pack**, **Microsoft Internet Server**, **Internet Service Manager.**



c) Select Internet Information Server

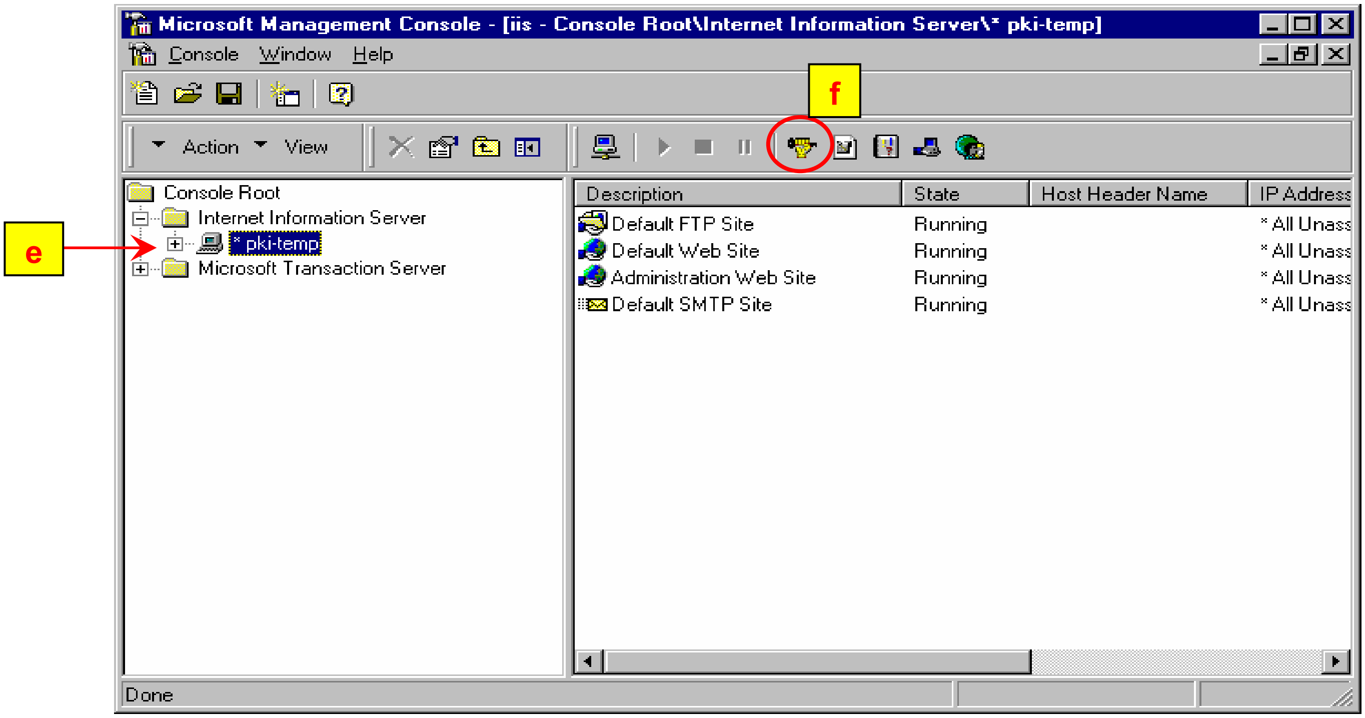

Microsoft Management Console - [iis - Console Root]
Console Window Help
Action View
Console Root
Internet Information Server
Microsoft Transaction Server
Ready
c

Name	Type
Internet Information Server	Snapin
Microsoft Transaction Server	Snapin

d) Double click or click on the '+'.

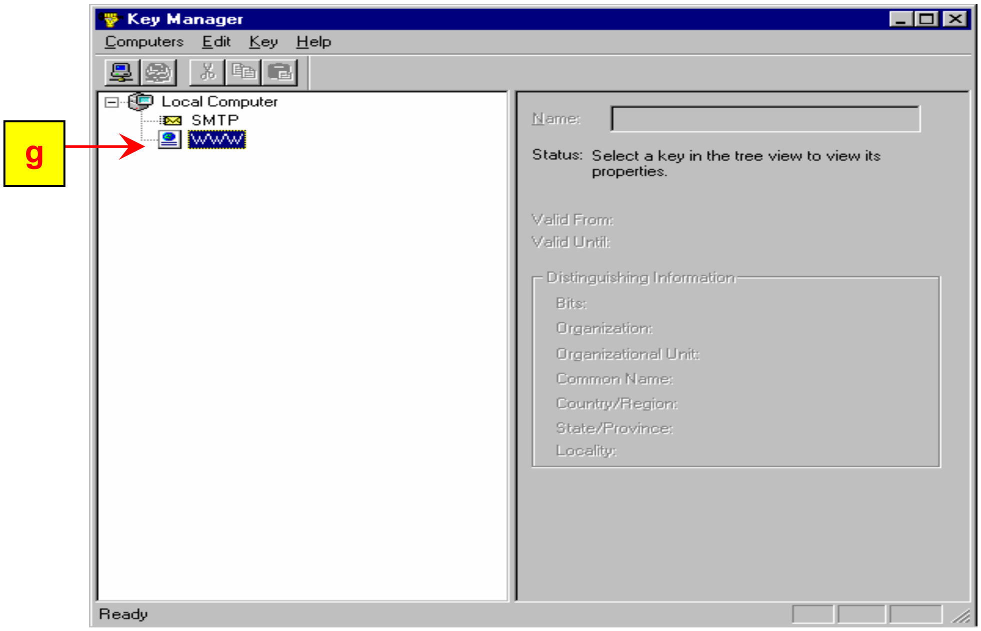
e) Select <server name>(ex. pki-temp)

f) Click on the **Key Manager** icon (resembles a hand holding a key).


Microsoft Management Console - [iis - Console Root\Internet Information Server* pki-temp]
Console Window Help
f
Action View
Console Root
Internet Information Server
* pki-temp
Microsoft Transaction Server
Done
e

Description	State	Host Header Name	IP Address
Default FTP Site	Running		* All Unass
Default Web Site	Running		* All Unass
Administration Web Site	Running		* All Unass
Default SMTP Site	Running		* All Unass

g) In the Key Manger window select **WWW**.

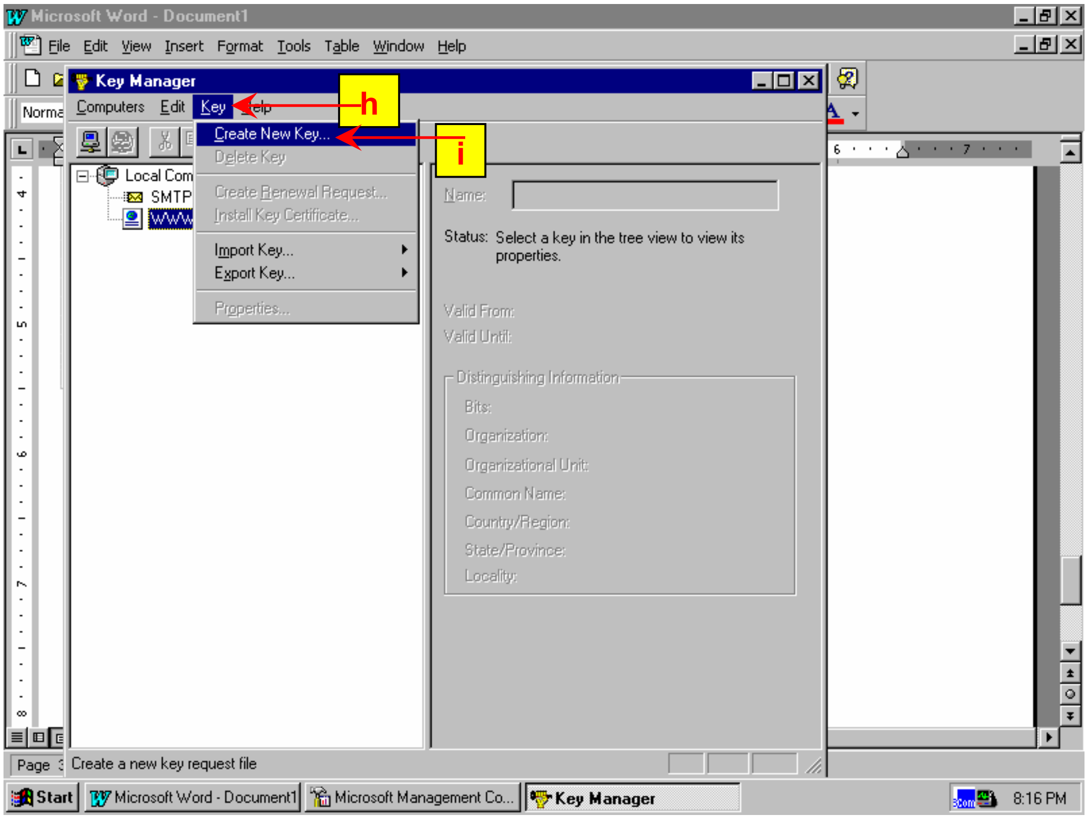


Status: Select a key in the tree view to view its properties.

Ready

h) Select the **Key** menu.

i) Select **Create New Key** (This will start the Key Wizard).



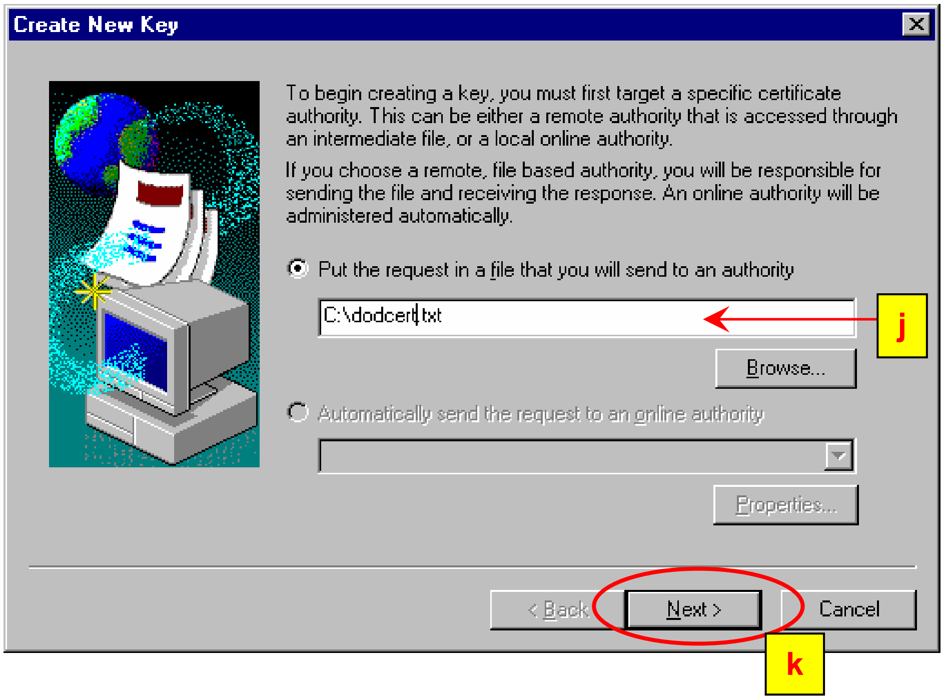
Status: Select a key in the tree view to view its properties.

Create a new key request file

The first window asks if the request will be placed into a file to send to a CA or will be sent automatically to an online CA. **Choose the first one** (request in a file).

j) Name the file **C:\dodcert.text**

k) Click **Next.**



Create New Key

To begin creating a key, you must first target a specific certificate authority. This can be either a remote authority that is accessed through an intermediate file, or a local online authority.

If you choose a remote, file based authority, you will be responsible for sending the file and receiving the response. An online authority will be administered automatically.

● Put the request in a file that you will send to an authority

C:\dodcert.txt

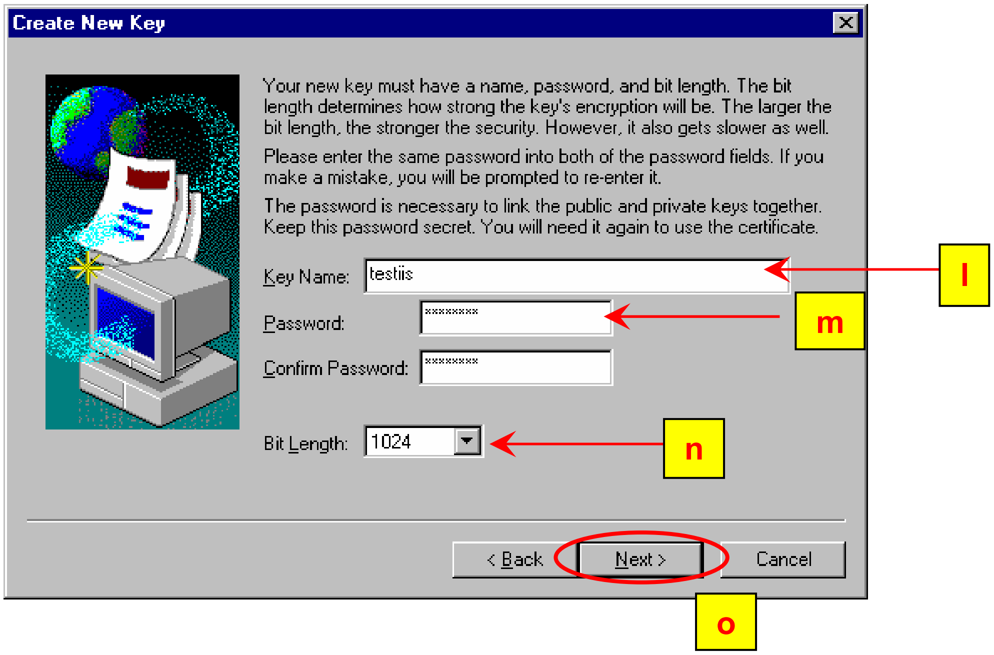
○ Automatically send the request to an online authority

l) Enter a name for the key (example is testis).

m) Create an 8-character password with at least one non-alphabetic character.

n) In the '**Bit Length**' field, **1024** must be selected.

o) Click **Next**.



Create New Key

Your new key must have a name, password, and bit length. The bit length determines how strong the key's encryption will be. The larger the bit length, the stronger the security. However, it also gets slower as well.

Please enter the same password into both of the password fields. If you make a mistake, you will be prompted to re-enter it.

The password is necessary to link the public and private keys together. Keep this password secret. You will need it again to use the certificate.

Key Name: testiis

Password: ********

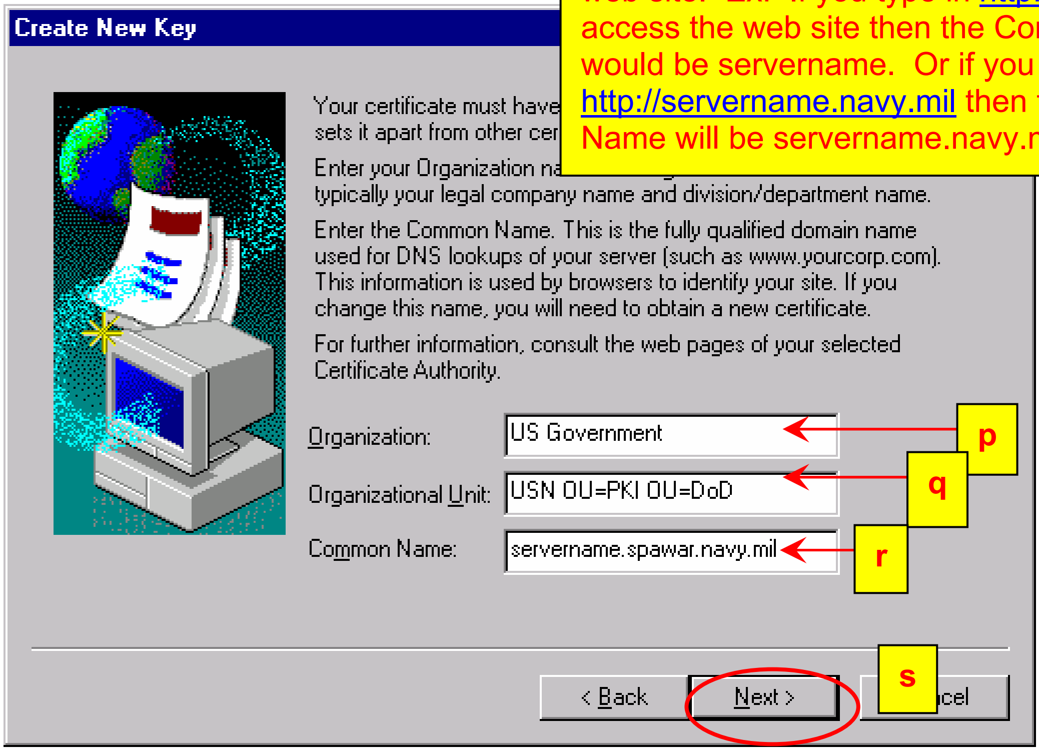
Confirm Password: ********

Bit Length: 1024

The next 3 screens asks for '*distinguished name*' information and *requestor's* information. It is important to ensure the validity of all the entered information. Certain information is required and will be put in bold text. IIS 4.0 does not allow commas.

- p) For *Organization*, enter **US Government**
- q) For *Organizational Unit*, enter **C/S/A ou=PKI ou=DoD** (ex. USN ou=PKI ou = DoD)
- r) For *Common Name*, enter the full name of the server. (ex. servername.spawar.navy.mil)
- s) Click **Next**.

Note: The Common Name must be the same name as the DNS Name typed in to access the web site. Ex: If you type in http://servername to access the web site then the Common Name would be servername. Or if you type in http://servername.navy.mil then the Common Name will be servername.navy.mil.



Create New Key

Your certificate must have
sets it apart from other cer

Enter your Organization na
typically your legal company name and division/department name.

Enter the Common Name. This is the fully qualified domain name used for DNS lookups of your server (such as www.yourcorp.com). This information is used by browsers to identify your site. If you change this name, you will need to obtain a new certificate.

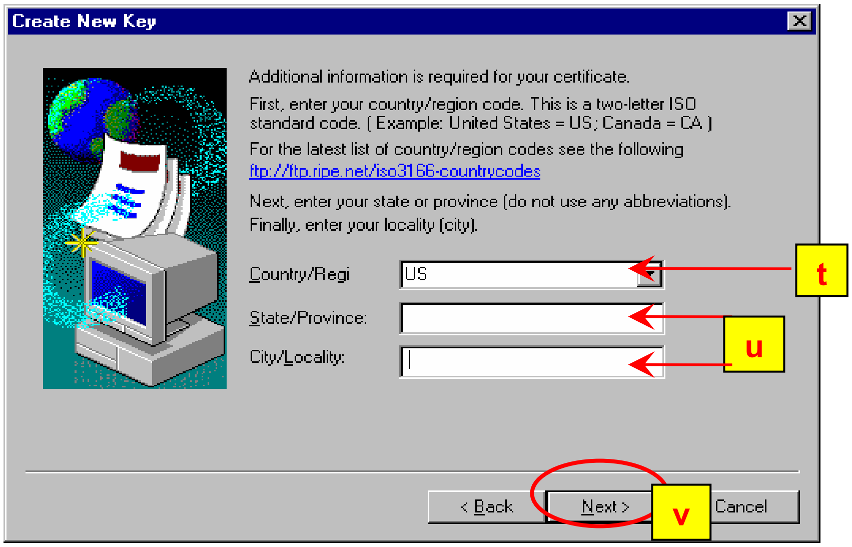
For further information, consult the web pages of your selected Certificate Authority.

Organization: US Government

Organizational Unit: USN OU=PKI OU=DoD

Common Name: servername.spawar.navy.mil

- t) For *Country/Region*, enter **US**
- u) *State/Province* and *City/Locality* must be blank, but IIS 4.0 doesn't allow for blanks so for each field, press the spacebar once.
- v) Click **Next.**



Create New Key

Additional information is required for your certificate.

First, enter your country/region code. This is a two-letter ISO standard code. (Example: United States = US; Canada = CA)

For the latest list of country/region codes see the following
ftp://ftp.ripe.net/iso3166-countrycodes

Next, enter your state or province (do not use any abbreviations). Finally, enter your locality (city).

Country/Regi: US

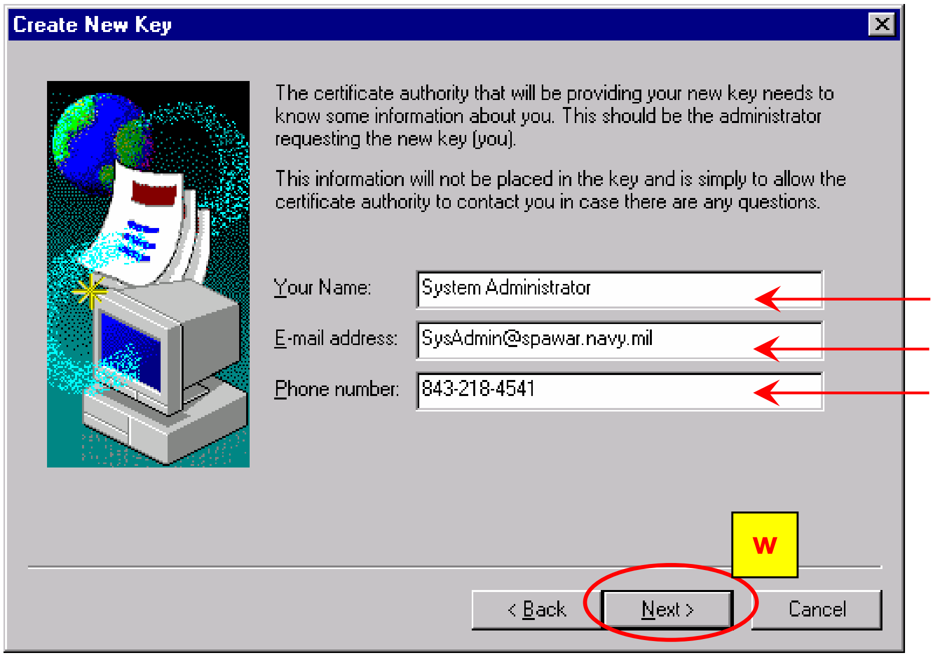
State/Province:

City/Locality:

Note: *State/Province* and *City/Locality* must be blank, but IIS 4.0 doesn't allow for blanks so for each field, press the spacebar once.

The following screen asks for the requestor's information. This is the Network System Administrator, Server Administrator, or LRA (Local Registration Authority). Must have a **valid email address** and **complete phone number**.

w) Click **Next**.



Create New Key

The certificate authority that will be providing your new key needs to know some information about you. This should be the administrator requesting the new key (you).

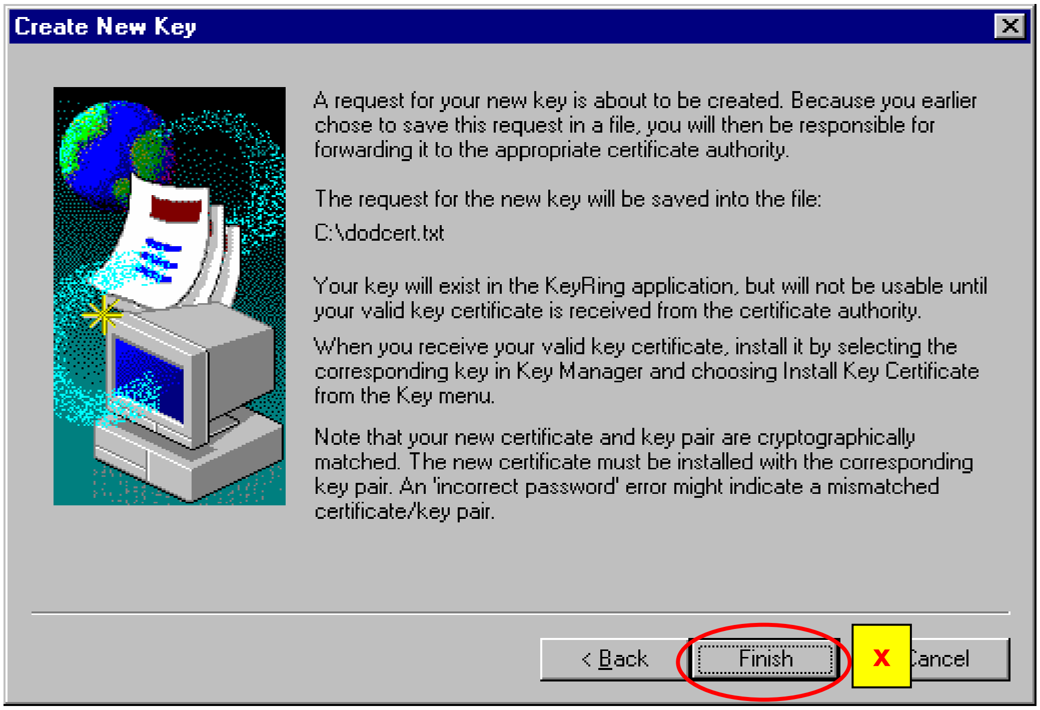
This information will not be placed in the key and is simply to allow the certificate authority to contact you in case there are any questions.

Your Name: System Administrator

E-mail address: SysAdmin@spawar.navy.mil

Phone number: 843-218-4541

x) Click **Finish**.



Create New Key

A request for your new key is about to be created. Because you earlier chose to save this request in a file, you will then be responsible for forwarding it to the appropriate certificate authority.

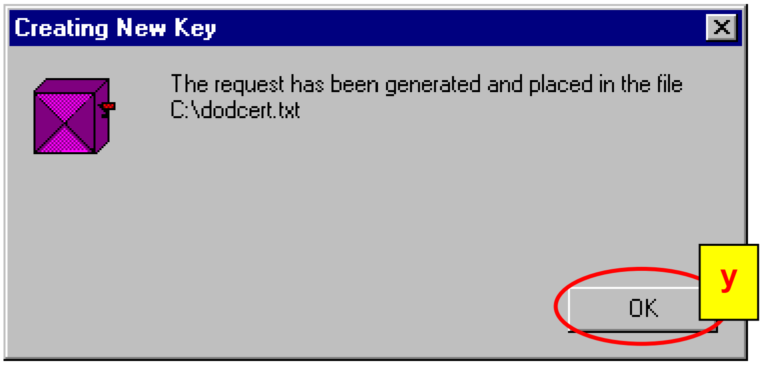
The request for the new key will be saved into the file:
C:\dodcert.txt

Your key will exist in the KeyRing application, but will not be usable until your valid key certificate is received from the certificate authority.

When you receive your valid key certificate, install it by selecting the corresponding key in Key Manager and choosing Install Key Certificate from the Key menu.

Note that your new certificate and key pair are cryptographically matched. The new certificate must be installed with the corresponding key pair. An 'incorrect password' error might indicate a mismatched certificate/key pair.

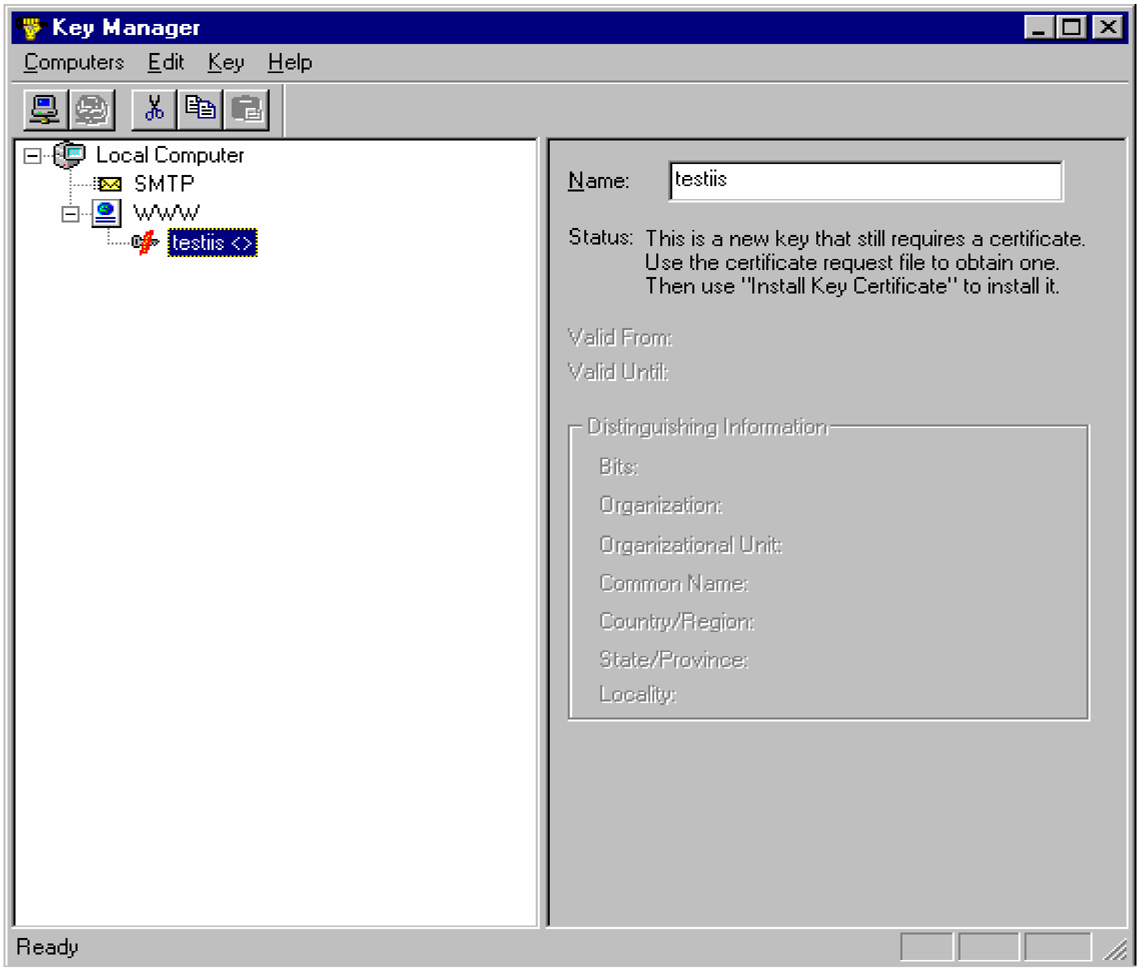
y) **Creating New Key** window will appear. Click **OK**.



Creating New Key

The request has been generated and placed in the file C:\dodcert.txt

The following screen will appear showing that the key has been tied to the WWW but is still unusable until the certificate is obtained and installed.



Key Manager

Name: testiis

Status: This is a new key that still requires a certificate. Use the certificate request file to obtain one. Then use "Install Key Certificate" to install it.

Valid From:

Valid Until:

Distinguishing Information

Bits:

Organization:

Organizational Unit:

Common Name:

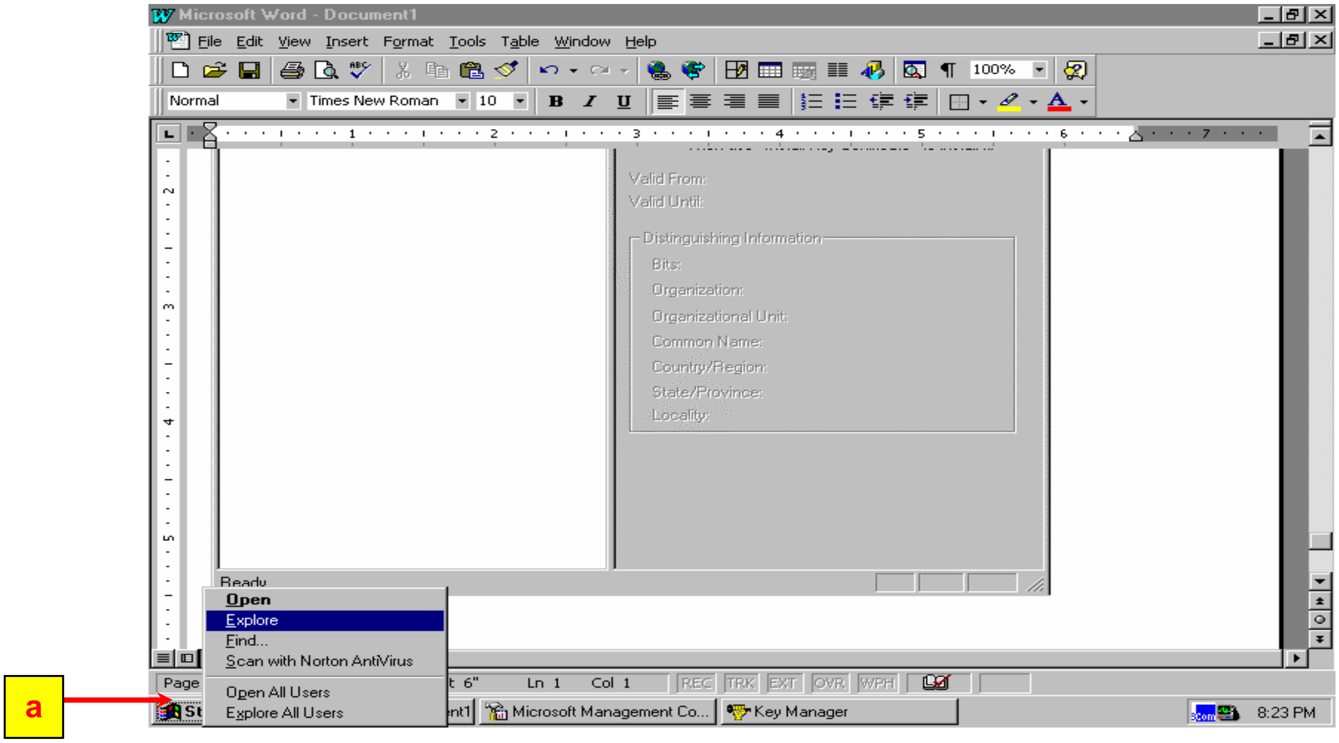
Country/Region:

State/Province:

Locality:

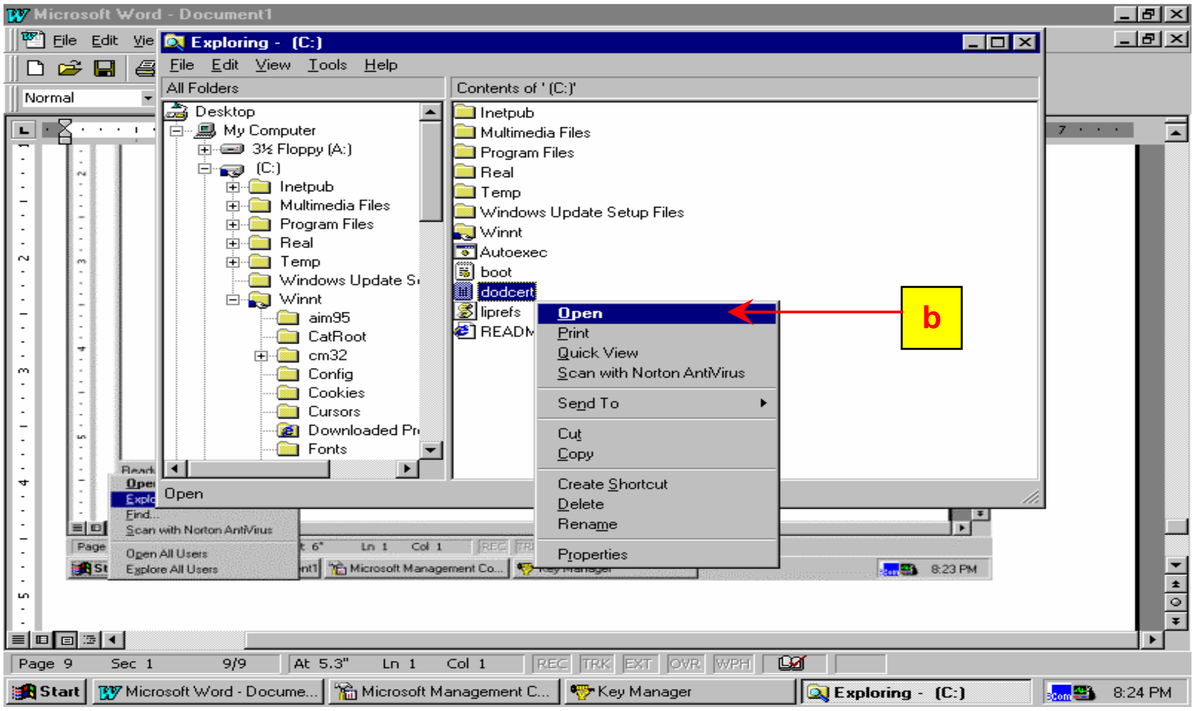
Ready

2. Requesting a Certificate.

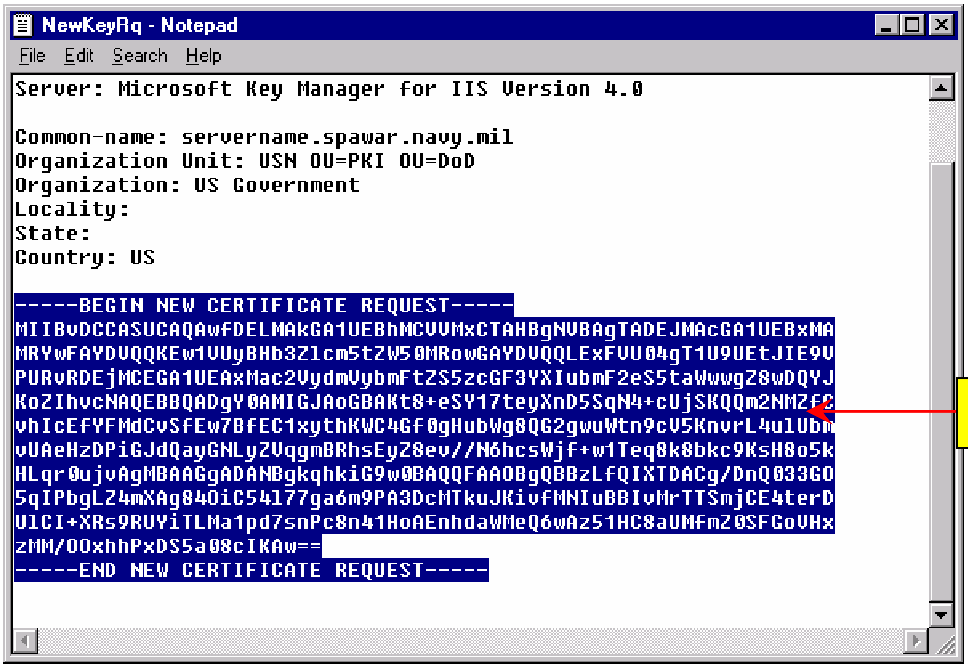

a
Microsoft Word - Document1
Open
Explore
Find...
Scan with Norton AntiVirus
Open All Users
Explore All Users
Microsoft Management Co...
Key Manager
8:23 PM

a) Start Windows NT Explorer by right-clicking the **Start** button and selecting **Explore**.

b) Open the file created in the previous section, **c:\dodcert.txt**. (Select the file, right-click, select **Open**).



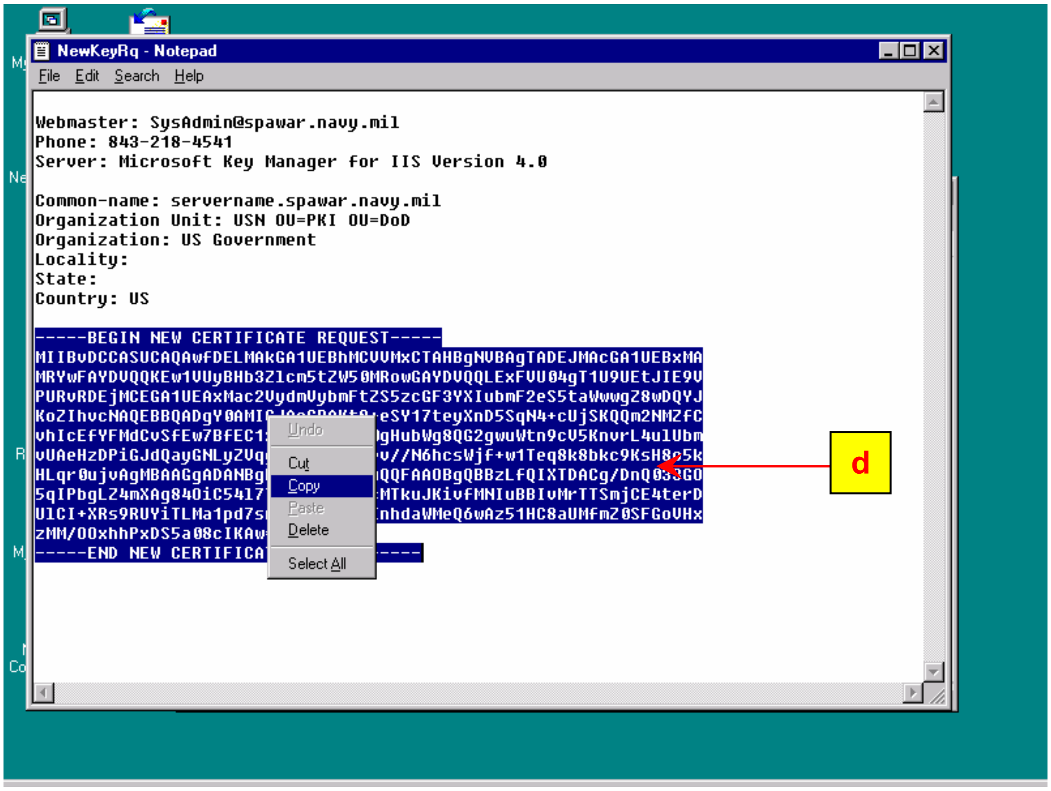
The file, **c:\dodcert.txt**, should appear like the screen below.



```
Server: Microsoft Key Manager for IIS Version 4.0

Common-name: servername.spawar.navy.mil
Organization Unit: USN OU=PKI OU=DoD
Organization: US Government
Locality:
State:
Country: US

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwFDELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMA
MRYwFAYDVQQKEw1VUyBHb3Zlcm5tZW50MRowGAYDVQQLExFVU04gT1U9UEtJIE9V
PURvRDEjMCEGA1UEAxMac2VydmVybmFtZS5zcGF3YXIubmF2eS5taWwwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKt8+eSY17teyXnD5SqN4+cUjSKQQm2NMZfC
vhIcEfYFMdCvSfEw7BfEC1xythKWC4Gf0gHubWg8QG2gwuWtn9cV5KnvrL4ulUbm
vUAeHzDPiGJdQayGNLyZVqgmBRhsEyZ8ev//N6hcsWjf+w1Teq8k8bkc9KsH8o5k
HLqr0ujvAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQBBzLfQIXTDACg/DnQ033GO
5qIPbgLZ4mXAg84OiC54l77ga6m9PA3DcMTkuJKivfMNIuBBIvMrTTSmjCE4terD
UlCI+XRs9RUYiTLMa1pd7snPc8n41HoAEnhdaWMeQ6wAz51HC8aUMfmZ0SFGoVHx
zMM/OOxhhPxDS5a08cIKAw==
-----END NEW CERTIFICATE REQUEST-----
```

c) Highlight the base-64 encoding to include **----------BEGIN NEW …** thru **END NEW…**

d) Copy the highlighted text to the clipboard.

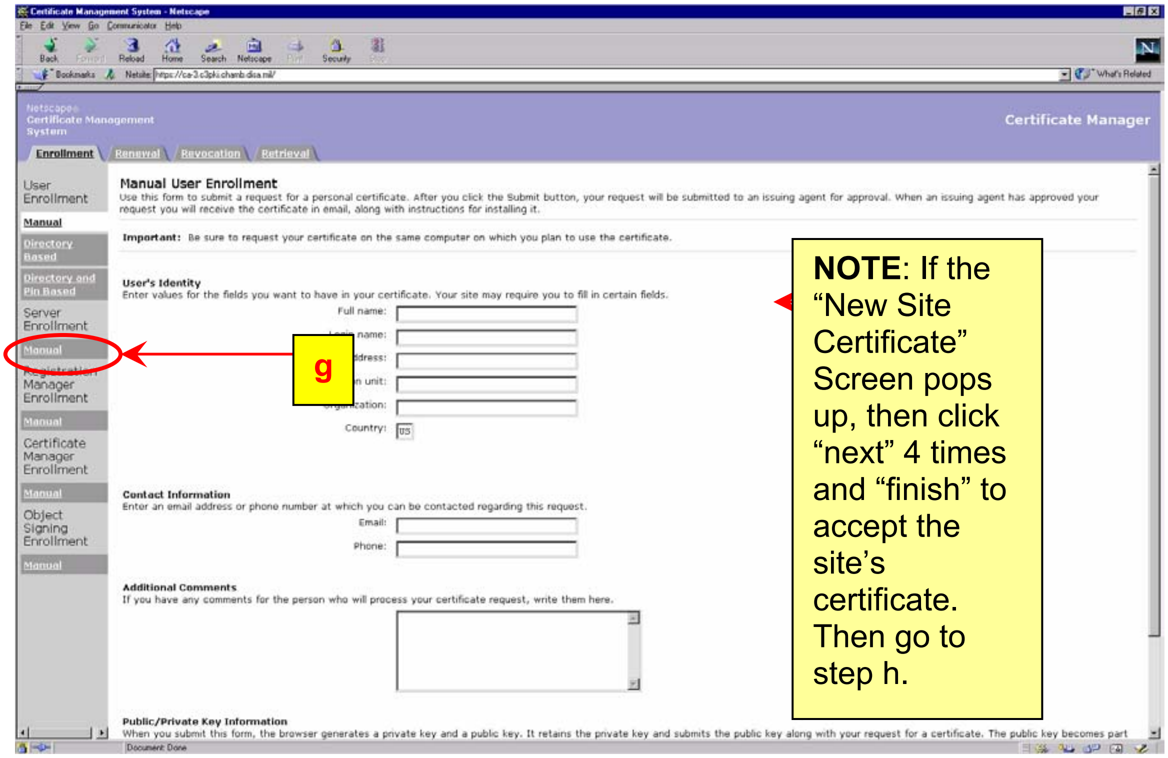


```
Webmaster: SysAdmin@spawar.navy.mil
Phone: 843-218-4541
Server: Microsoft Key Manager for IIS Version 4.0

Common-name: servername.spawar.navy.mil
Organization Unit: USN OU=PKI OU=DoD
Organization: US Government
Locality:
State:
Country: US

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwFDELMAkGA1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMA
MRYwFAYDVQQKEw1VUyBHb3Zlcm5tZW50MRowGAYDVQQLExFVU04gT1U9UEtJIE9V
PURvRDEjMCEGA1UEAxMac2VydmVybmFtZS5zcGF3YXIubmF2eS5taWwwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMI          eSY17teyXnD5SqN4+cUjSKQQm2NMZfC
vhIcEfYFMdCvSfEw7BfEC1          gHubWg8QG2gwuWtn9cV5KnvrL4ulUbm
vUAeHzDPiGJdQayGNLyZVq          v//N6hcsWjf+w1Teq8k8bkc9KsH8o5k
HLqr0ujvAgMBAAGgADANBg          QQFAAOBgQBBzLfQIXTDACg/DnQ033GO
5qIPbgLZ4mXAg84OiC5417          MTkuJKivfMNIuBBIvMrTTSmjCE4terD
UlCI+XRs9RUYiTLMa1pd7s          nhdaWMeQ6wAz51HC8aUMfmZ0SFGoVHx
zMM/OOxhhPxDS5a08cIKAw
-----END NEW CERTIFICA          -----
```

e) Start **Netscape or Internet Explorer** (which ever is preferred).

f) Go to site https://ca-3.c3pki.chamb.disa.mil**.** See Note below.

g) Select **Manual** under Server Enrollment option.


Certificate Management System - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Bookmarks Netsite: https://ca-3.c3pki.chamb.disa.mil/
What's Related
Netscape Certificate Management System
Certificate Manager
Enrollment
Renewal
Revocation
Retrieval
User Enrollment
Manual
Directory Based
Directory and Pin Based
Server Enrollment
Manual
Registration Manager Enrollment
Manual
Certificate Manager Enrollment
Manual
Object Signing Enrollment
Manual
g
Document: Done

Manual User Enrollment

Use this form to submit a request for a personal certificate. After you click the Submit button, your request will be submitted to an issuing agent for approval. When an issuing agent has approved your request you will receive the certificate in email, along with instructions for installing it.

Important: Be sure to request your certificate on the same computer on which you plan to use the certificate.

User's Identity

Enter values for the fields you want to have in your certificate. Your site may require you to fill in certain fields.

Full name:

name:

ddress:

n unit:

zation:

Country: US

Contact Information

Enter an email address or phone number at which you can be contacted regarding this request.

Email:

Phone:

Additional Comments

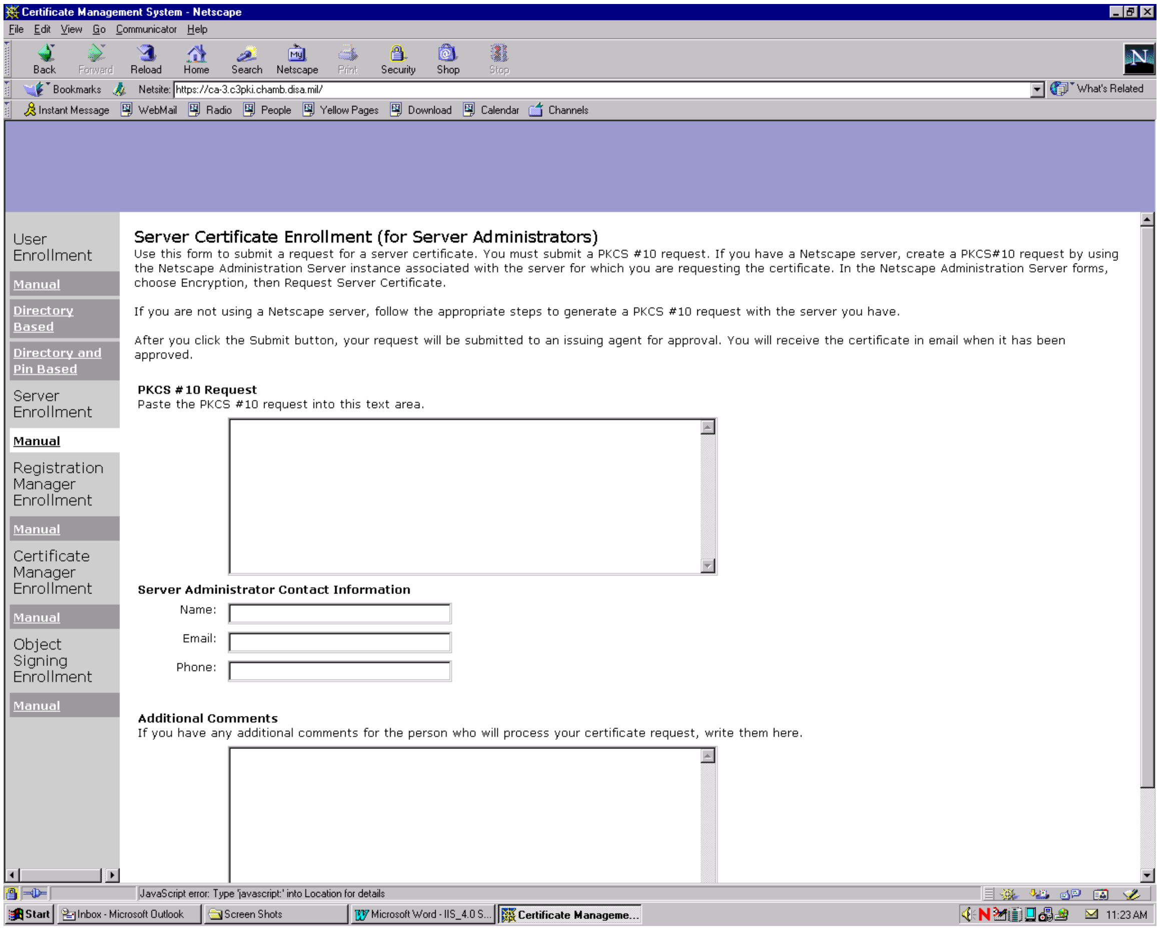
If you have any comments for the person who will process your certificate request, write them here.

Public/Private Key Information

When you submit this form, the browser generates a private key and a public key. It retains the private key and submits the public key along with your request for a certificate. The public key becomes part

NOTE: If the "New Site Certificate" Screen pops up, then click "next" 4 times and "finish" to accept the site's certificate. Then go to step h.

The “*Server Certificate Enrollment*” will appear.


Certificate Management System - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: https://ca-3.c3pki.chamb.disa.mil/ What's Related
Instant Message WebMail Radio People Yellow Pages Download Calendar Channels
User Enrollment
Manual
Directory Based
Directory and Pin Based
Server Enrollment
Manual
Registration Manager Enrollment
Manual
Certificate Manager Enrollment
Manual
Object Signing Enrollment
Manual
JavaScript error: Type 'javascript:' into Location for details
Start Inbox - Microsoft Outlook Screen Shots Microsoft Word - IIS_4.0 S... Certificate Manageme...
11:23 AM

Server Certificate Enrollment (for Server Administrators)

Use this form to submit a request for a server certificate. You must submit a PKCS #10 request. If you have a Netscape server, create a PKCS#10 request by using the Netscape Administration Server instance associated with the server for which you are requesting the certificate. In the Netscape Administration Server forms, choose Encryption, then Request Server Certificate.

If you are not using a Netscape server, follow the appropriate steps to generate a PKCS #10 request with the server you have.

After you click the Submit button, your request will be submitted to an issuing agent for approval. You will receive the certificate in email when it has been approved.

PKCS #10 Request

Paste the PKCS #10 request into this text area.

Server Administrator Contact Information

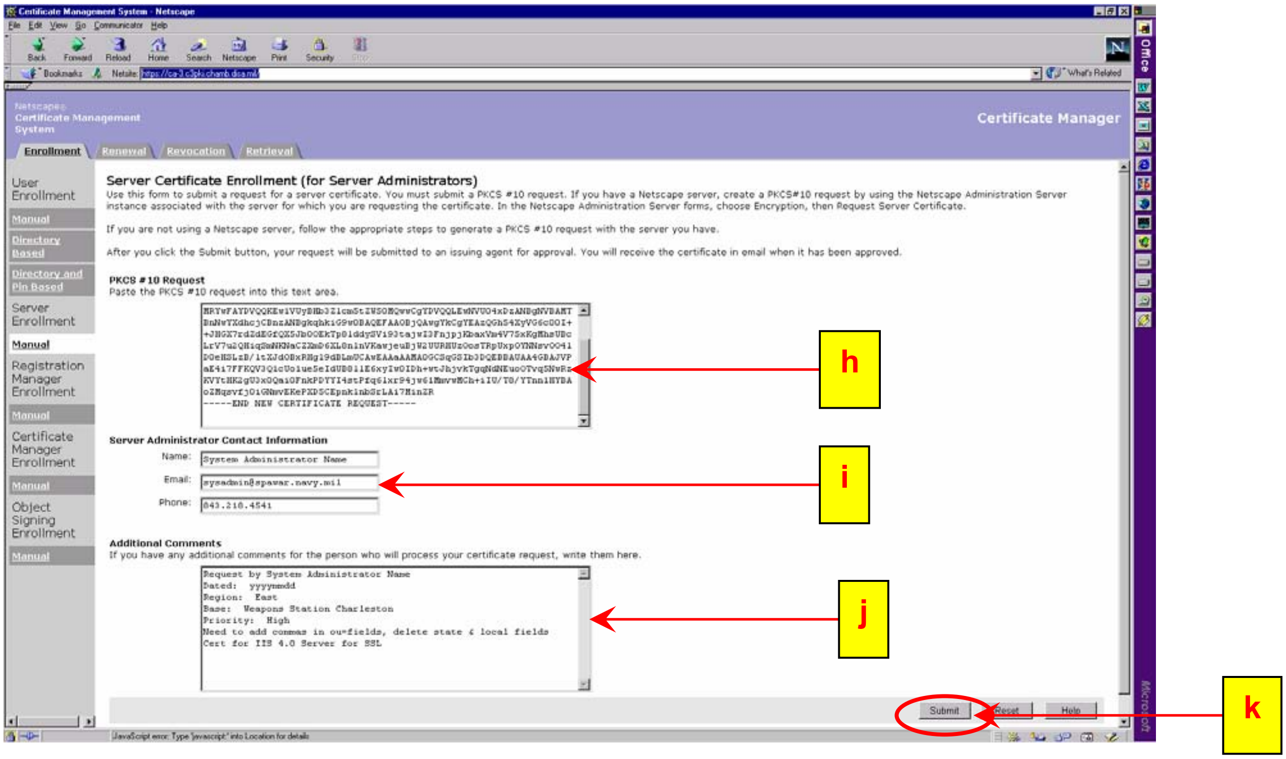
Name:

Email:

Phone:

Additional Comments

If you have any additional comments for the person who will process your certificate request, write them here.


Certificate Management System - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: https://ca-3.c3pki.chamb.disa.mil/
What's Related
Netscape® Certificate Management System
Certificate Manager
Enrollment Renewal Revocation Retrieval
User Enrollment
Manual
Directory Based
Directory and Pin Based
Server Enrollment
Manual
Registration Manager Enrollment
Manual
Certificate Manager Enrollment
Manual
Object Signing Enrollment
Manual
Submit Reset Help
JavaScript error: Type 'javascript:' into Location for details
h
i
j
k

Server Certificate Enrollment (for Server Administrators)

Use this form to submit a request for a server certificate. You must submit a PKCS #10 request. If you have a Netscape server, create a PKCS#10 request by using the Netscape Administration Server instance associated with the server for which you are requesting the certificate. In the Netscape Administration Server forms, choose Encryption, then Request Server Certificate.

If you are not using a Netscape server, follow the appropriate steps to generate a PKCS #10 request with the server you have.

After you click the Submit button, your request will be submitted to an issuing agent for approval. You will receive the certificate in email when it has been approved.

PKCS #10 Request

Paste the PKCS #10 request into this text area.

```
MRYwFAYDVQQKEwiVUyBHb3ZlcmStIW5OMQwwCgYDVQQLEwNVU04xDzANBgNVBAMT
BnNwYXdhcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzQGhS4XyVG6c0OI+
+JHGX7rdZdEGfQX5JbOOEkTp0lddySVi93tajwI3FnjpjKbaxVm4V75xKgMhsUBc
LrV7u2QHiqSmNKNaCZXmD6XL0n1nVKawjeuBjW2UURHUzOosTRpUxpOYNNsvOO41
DOeHSLzB/1tXJdOBxRHg19dBLmUCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAJVP
aE4i7FFKQV3QicUo1ue5eIdUB011E6xyIwOIDh+wtJhjvkTgqNdNEuoOTvq5NwRz
KVYtHK2gU3xOQai0FnkPDYYI4stPfq6lxr94jw61MmvwMCh+iIU/T0/YTnn1HYBA
oZMqsvfj0iGNmvEKePXDSCEpnk1nbGrLAi7MinZR
-----END NEW CERTIFICATE REQUEST-----
```

Server Administrator Contact Information

Name: System Administrator Name

Email: sysadmin@spawar.navy.mil

Phone: 843.218.4541

Additional Comments

If you have any additional comments for the person who will process your certificate request, write them here.

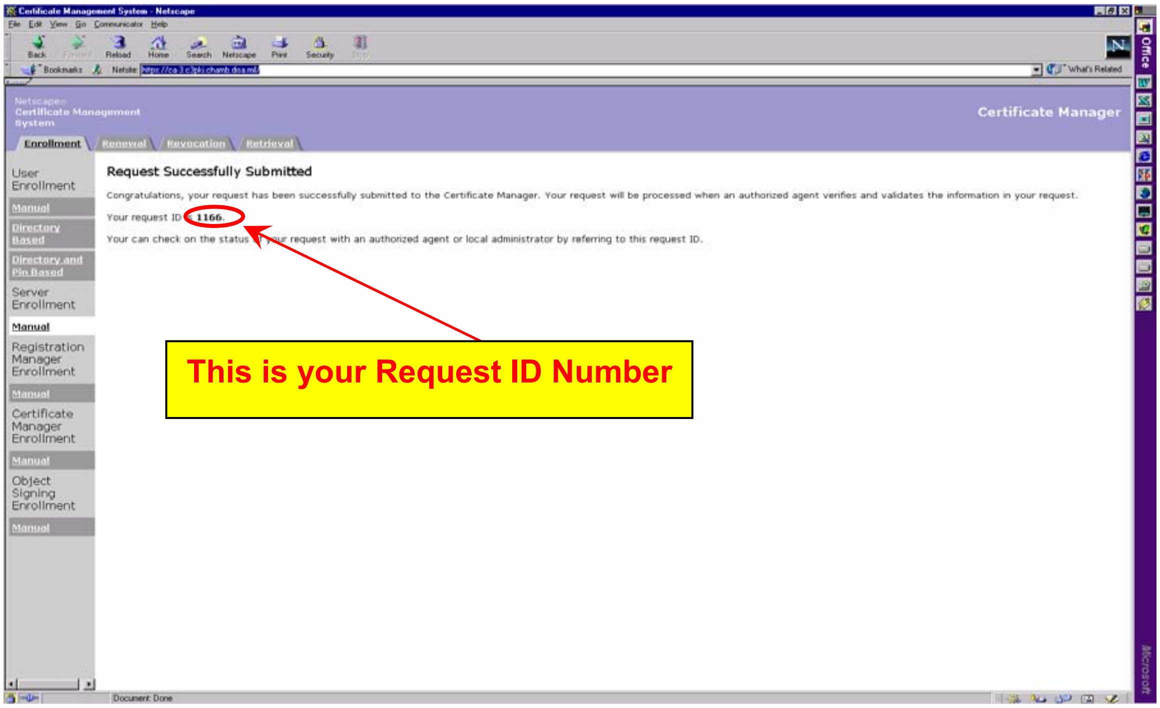
```
Request by System Administrator Name
Dated:  yyyymmdd
Region:  East
Base:  Weapons Station Charleston
Priority:  High
Need to add commas in ou=fields, delete state & local fields
Cert for IIS 4.0 Server for SSL
```

h) Paste the base-64 encoding into the box labeled PKCS #10 Request.
i) Fill out the **Contact Info** fields.
j) In the **Additional Comments to Issuing Agent** text box, follow the example below.

Request by System Administrator Name
Date: yyyymmdd
Region: East Coast, West Coast
Base: Base Name
Priority: High/Low
Need to add commas to 'ou' field and must delete the 'L' & 'St' fields from the CN.
Justification: To enable SSL on the web server and/or for client authentication.
**All text shown in bold is to be entered exactly as shown. All other text is to be replaced with appropriate information as it pertains to your server/site.

k) Click **Submit Request**.

A confirmation page, ‘Request Successfully Submitted’ will contain request ID number. **Print this page**, if possible. If not, **retain the request ID number** some other way. It will be required to continue the certificate request process. An example Server Certificate Signing Request is shown on the next page.


Certificate Management System - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: https://ca-3.c3pki.chamb.disa.mil/
What's Related
Netscape Certificate Management System
Certificate Manager
Enrollment Renewal Revocation Retrieval
User Enrollment
Manual
Directory Based
Directory and Pin Based
Server Enrollment
Manual
Registration Manager Enrollment
Manual
Certificate Manager Enrollment
Manual
Object Signing Enrollment
Manual
Document: Done
Office
Microsoft

Request Successfully Submitted

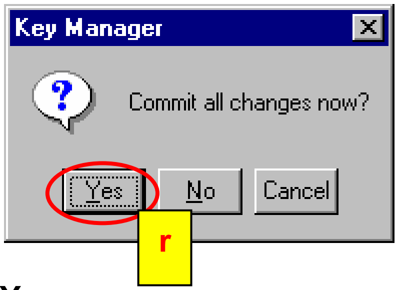
Congratulations, your request has been successfully submitted to the Certificate Manager. Your request will be processed when an authorized agent verifies and validates the information in your request.

Your request ID is 1166.

Your can check on the status of your request with an authorized agent or local administrator by referring to this request ID.

This is your Request ID Number

l) Close the browser.
m) Close the notepad window.
n) Close IIS windows.



Commit all changes now?

o) Click **Yes**.
p) Click **Yes** on ‘*Change Settings to Console*’ window.

3. Approval Notification.

a. The next step in the Server Certificate Request Process involves sending an email to Inga George, georgei@spawar.navy.mil identifying by the request ID number produced at the end of the last section that the certificate request is ready for review. The email must contain the following **(everything in bold is to be typed as shown** with the rest of the information being replaced with what is appropriate for each individual server):

Reference Number: xxxx (with xxxx being the request ID number received from the last section)
Host Name: www.sample.navy.mil (this is an example only)
IP Address: 102.21.12.12 (the server's ip address)
Region: East Coast
Base: Base Name
Network System Administrator (NSA): Sgt John Doe
System Owner: JFCOM
Security Level: SBU (Sensitive But Unclassified)
Applications on Server: Development versions of the following:
1) SPAWAR PKI Home Page
2) INFOSEC Home Page

Certification Justification/Requirements:

- To enable SSL on the server.

a. The LRA/RA, upon receipt of the email, will review the request. If the request was done correctly and is approved, the LRA/RA will send an email that will contain a *Certificate Serial Number (CSN)*. The CSN must be utilized in order to download the certificate. If the request is not approved, the RA will notify the requestor/LRA why.

b. If the requestor does not receive anything from the LRA/RA within 1 week after the email was sent, contact the LRA/RA by phone. The number is comm (843) 218-5574 or DSN 588-5574.

c. When the email with the CSN has been received, refer to "Server Certificate Enabling for Microsoft Internet Information Server 4.0 Step 2: Obtaining/Installing PKI Server Certificate." If you do not receive a copy of this document within 2 days of receiving the CSN, please contact Inga George, georgei@spawar.navy.mil.